Cassandra Crossing/ La prevedibile banalità del Male

(498) —E' davvero così difficile, nella guerra cibernetica, "spegnere" l'Internet via satellite?

Cassandra Crossing/ La prevedibile banalità del Male
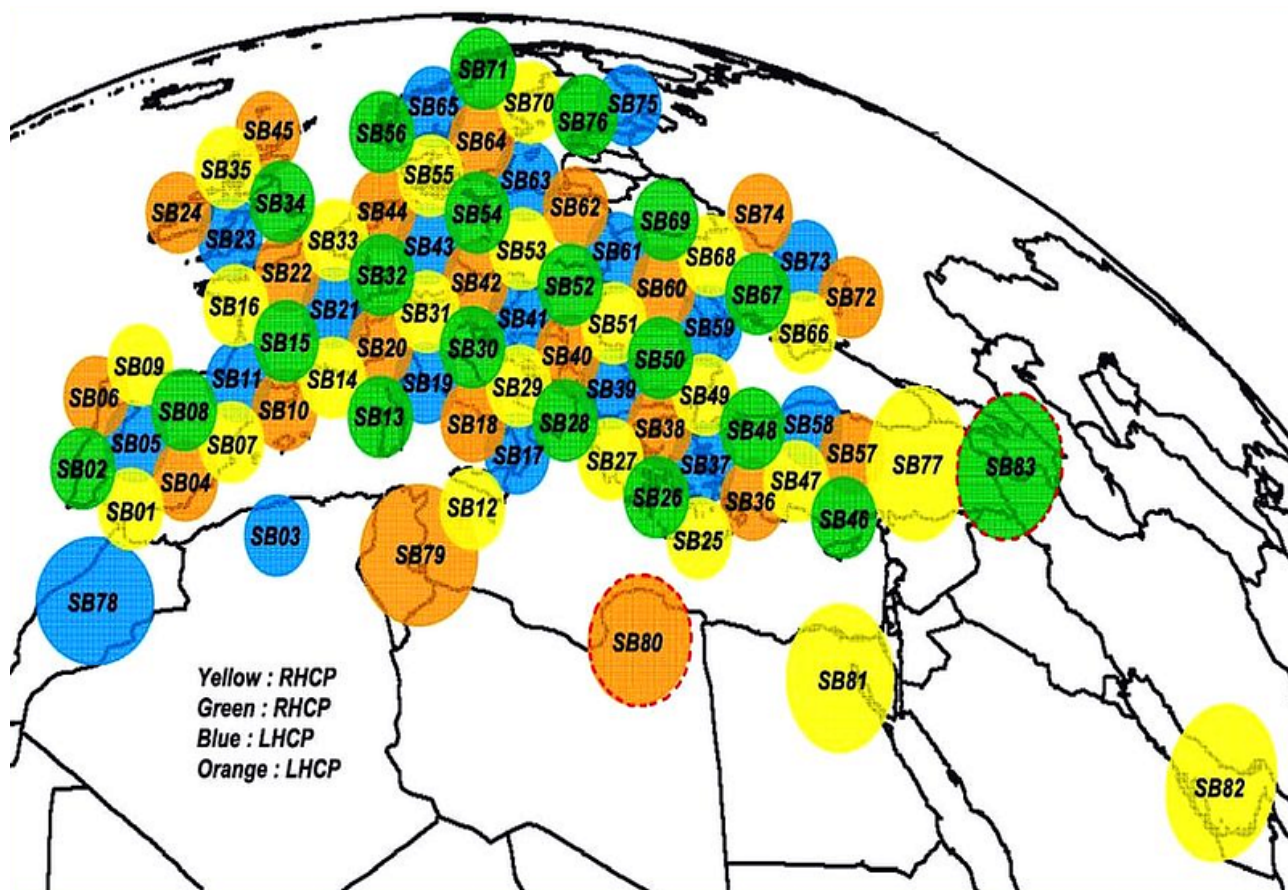
Figure 1:

(498)—E' davvero così difficile, nella guerra cibernetica, "spegnere" l'Internet via satellite?

21 marzo 2022—Cassandra si è fatta un'idea abbastanza esatta di un probabile atto di guerra cibernetica, tanto da decidere di esternare la sua opinione a beneficio dei suoi 24 indefessi lettori.

Si tratta del blackout di alcune decine di migliaia di utenze di internet satellitare VIASAT (distribuite sotto vari nomi commerciali), in alcuni paesi europei inclusa l'Ucraina, che è avvenuta proprio all'inizio delle ostilità.

Fonti ufficiali riferiscono che un certo numero di modem satellitari, variabile da una fonte all'altra ma sempre dell'ordine delle 10.000 unità, sono stati resi non operativi, e dovranno "probabilmente" essere sostituiti.

Pur essendo questa una descrizione abbastanza esatta, è rivestita di quell'aurea mistica di tecnologie e segreto, che, come la *Terza legge di Clarke* enuncia, la rende indistinguibile dalla magia.

Allora vediamo se Cassandra riesce ad alzare il velo, e spiegare come non di armi ultrascientifiche si tratti, ma di pura e semplice ordinarietà e vetustà delle architetture hardware e software, oltre che ovviamente della naturale tendenza a risparmiare dovunque sia possibile, e della normale dose di errori ed omissioni propria dell'industria.

Una premessa, nel caso fosse necessario; Cassandra non è in possesso di nessuna informazione riservata, ma sa solo utilizzare, con competenza vicina alla media, i motori di ricerca ed i forum.

Non è neppure aggiornata sullo stato dell'arte di tecnologie moderne e/o proprietarie, ma possiede una certa esperienza, anche se ormai vetusta, di sviluppo industriale di hardware e software.

Non serve di più. Partendo da questi elementi, Cassandra può spiegare, e banalizzare, un evento che, lungi da essere misterioso, è eccitante e sofisticato quanto una scodella di semolino od un DDOS di basso livello.

E vendemmiando tra i moltissimi modi di compromettere un modem satellitare, ben elencati in questo post, può ipotizzare cosa è successo veramente.

Quindi, insieme ai 24 intraprendenti lettori, partiamo da zero.

Qualunque modem, anzi qualunque oggetto informatico, possiede un firmware, cioè un software, anche molto complesso, memorizzato permanentemente in un componente hardware del circuito stampato.
Può trattarsi anche di una semplice scheda uSD, come quelle che si usano per espandere la memoria degli smartphone, o di componenti hardware più sofisticati e specializzati.

Poco conta, perché il fatto importante è che questo software, insieme al componente che lo contiene, viene rinchiuso in una scatola, magari elegante e certamente dotata di prese e lucine, e la scatola viene installata da qualche parte.
Nel nostro caso, trattandosi di connessioni Internet satellitari, probabilmente un posto assai fuori mano, magari al freddo ed in alto.

Ed il firmware dovrebbe ovviamente poter essere aggiornato senza aprire la scatola, senza che un tecnico debba collegarvi il suo laptop, possibilmente senza alcun intervento manuale, magari in maniera totalmente automatica, con una singola operazione.

Per caricare la prima volta un firmware si possono usare vari metodi, ma in generale sul circuito stampato di qualunque apparecchiatura di questo tipo è presente un connettore JTAG; si tratta di uno *standard industriale* che permette di programmare componenti programmabili in maniera standard (bello, vero?). Lasciate perdere ed andiamo avanti

Tanto potente e temuto è il connettore JTAG che normalmente viene usato soltanto durante lo sviluppo o la riparazione, mentre nelle apparecchiature destinate alla vendita non è accessibile (manca il foro nella scatola), e spesso non viene neppure saldato il connettore sul circuito stampato, ma viene lasciato il posto vuoto.

Croce e delizia degli smanettoni hardware di qualche anno fa era appunto aprire la scatola, individuare il punto esatto del circuito stampato dove avrebbe dovuto essere montato il connettore JTAG e saldarci due fili, diretti verso un opportuno adattatore USB. E le magie degli smanettoni potevano iniziare!

Durante il normale funzionamento il firmware non viene ovviamente aggiornato in questo modo, ma piuttosto (l'avrete fatto almeno una volta sul modem casalingo) utilizzando l'interfaccia web del modem stesso, scaricando il firmware aggiornato dal sito del produttore e scrivendolo dentro il componente apposito con un semplice click su un pulsante.

Tutti gli oggetti appena più moderni, per esempio gli oggetti IoT casalinghi, fanno o possono fare questa operazione in maniera totalmente automatica ed invisibile all'utente.

Torniamo ai nostri modem satellitari,
Tutte le apparecchiature che comunicano via radio, vedi caso i modem satellitari, ma anche molti comuni televisori, posseggono la possibilità di scaricare un firmware che viene trasmesso via radio.

Quale miglior sistema di questo per uno scatolotto installato in località remote? I modem utilizzati da Viasat sono appunto dotati di questa capacità.

Il caricamento del firmware viene ovviamente controllato da un sistema di distribuzione, che è in parte vincolato dalle architetture dei sistemi satellitari; sono architetture in cui si cerca di sgravare di tutta la complessità possibile il satellite (decisamente più difficile da aggiornare!), concentrandola per quanto possibile nel software delle stazioni terrestri.

Il problema di distribuire in maniera affidabile e sicura il firmware è da tempo risolto a livello industriale con vari metodi, che contrastano però con i costi, con i vincoli di architetture software vecchie, e con i limiti dell'hardware.
Questo spesso porta a soluzioni ricche di chiavi crittografiche da aggiornare manualmente, od addirittura incorporate nel software, ed altre "delizie" simili. Persino i moderni sistemi d'arma sono gestiti così, quindi non c'è da meravigliarsi.

Avventuriamoci adesso, armati del solo *rasoio di Occam*, nel campo delle ipotesi.

Ci basta questo strumento per fare un'ipotesi semplice e banale che spiega perfettamente l'evento; si è trattato della compromissione del sistema di aggiornamento dei firmware di una singola stazione terrestre, e di un singolo comando che ha caricato una versione "malevola" del firmware sull'intera "flotta" di modem.

Un firmware, malevolo o meno, al momento del boot ha il il pieno controllo sull'hardware; può limitarsi a non funzionare, non permettere ulteriori aggiornamenti e stare li in eterno, o più efficacemente sovrascrivere il bootloader (l'equivalente del Master Boot Record) della scheda, e bloccare permanentemente il modem, impedendone il riavvio.

I modem possono essere dotati di accorgimenti volte ad evitare queste situazioni, come una seconda copia del firmware in sola lettura, che permetta solo di aggiornare il firmware, ma sono accorgimenti che costano, non sempre sono presenti, non sempre, anche se presenti, possono essere utilizzati, e non sempre vengono poi effettivamente utilizzati.

Non si tratta quindi di un attacco distruttivo; il modem è integro ed il firmware, andando sul posto per ogni modem, si potrebbe ricaricare, copiando l'intero filesystem virtuale via JTAG se ci fosse il connettore, che non c'è, e quindi aprendo la scatola e saldandone uno al circuito stampato.

I costi di una simile procedura sono però improponibili; è molto meno costoso spedire un modem nuovo all'utente e farlo sostituire a lui. Ma chi ha oggi 10.000 modem pronti per la spedizione in magazzino? E che dire della logistica per farli arrivare in zona di guerra?

Ecco che la negazione di una infrastruttura critica in un momento ed una zona ancora più critici può essere spiegata con un tipo di attacco, ahimè di "ordinaria amministrazione" nel mondo della sicurezza informatica, affascinante appunto come una scodella di semolino.

Ma resta il fatto, provato e confermato, che qualcuno, in qualche modo, ha veramente "ucciso" l'internet satellitare in una zona di guerra.

Ed è stato veramente troppo facile.

UPDATE: durante la lunga gestazione di questo articolo, Viasat ha “*ammesso*” , che le cose sono andate proprio così; dalla vostra profetessa preferita non potevate aspettarvi niente di meno!

UPDATE: il CEO di Viasat conferma implicitamente che il problema è un firmware alterato, e fornisce particolari sulla logistica che confermano anche i dettagli “*vaticinati*” da Cassandra.

Viasat chair Mark Dankberg told a satellite conference that … “thousands of modems were taken offline. In most of the cases of the modems that went offline, they need to be replaced. They can be refurbished, so we’re recycling modems through,”.

L’amministratore delegato di Viasat Mark Dankberg ha dichiarato ad una conferenza sui satelliti che “… migliaia di modem sono stati messi offline e devono essere sostituiti. Essi possono essere riparati, così li stiamo riciclando.”

By Marco A. L. Calamari on March 24, 2022.

Canonical link

Exported from Medium on August 27, 2025.